



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/576,393	04/20/2006	Josephus Arnoldus Henricus Kahlman	NL031296	2424
24737 7590 04/20/2009 PHILIPS INTELLECTUAL PROPERTY & STANDARDS P.O. BOX 3001 BRIARCLIFF MANOR, NY 10510				
EXAMINER				
POPHAM, JEFFREY D				
ART UNIT		PAPER NUMBER		
2437				
MAIL DATE		DELIVERY MODE		
04/20/2009		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/576,393

**Applicant(s)**

KAHLMAN ET AL.

**Examiner**

JEFFREY D. POPHAM

**Art Unit**

2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 30 January 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 April 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-8508)
- Paper No(s)/Mail Date \_\_\_\_\_

- 4) ☐ Interview Summary (PTO-413)
- Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

***Remarks***

Claims 1-13 are pending.

***Response to Arguments***

1. Applicant's arguments filed 1/30/2009 have been fully considered but they are not fully persuasive.

Applicant argues that "The claims are not believed to be narrowed in scope", however, the claims have been narrowed in that they now define the delay means as comprising an analog noise source (claim 1, for example). It is first noted that the term analog or variations thereof only appears once in the instant application, as filed. This reference may be found at the bottom of page 2, stating that "It was found that adding a noise to the responded (generally analogue) data from the memory increases an integration time for producing reliable (generally digital) data." Furthermore, this is the sole time that digital is referred to. However, the application as originally filed does not describe that the noise source must be analog. Page 4, lines 6-8, for example, recite that "the integrated circuit comprises a noise source 3 generating a noise signal which is added to the response signal outputted from the look-up table 2 by an adder 4." As one can see, this noise source is not analog, but rather, is merely capable of generating a noise signal that is added to a response. While a noise source may include an analog component (such as, for example, components described with respect to figure 2), the noise source of the instant application need not always be an analog component. As can be seen in the description of figure 1, the noise

Art Unit: 2437

source is merely described as "a noise source 3" and does not designate such a source as being analog, digital, or in any other manner. Therefore, in the previous set of claims, "delay means" could clearly be either analog or digital, or a combination of the two. Therefore, the claims have been narrowed by explicitly defining the delay means as "comprising an analog source for adding a noise signal...".

Applicant also argues that amended claim 11 has support in the application as originally filed, however, as will be described below, it does not.

Applicant argues, with respect to claim 13, that "the analog approaches taught by the invention are far more robust than the digital methods taught in Silverbrook." However, claim 13 recites no strictly analog components. As described above, "delay means" could comprise either digital, analog, or a combination of the two in the instant invention. Claim 13 does recite "a noisy read-out amplifier", however, as is known in the art, an amplifier may be digital, and need not be analog. Furthermore, since Silverbrook teaches such a noisy read-out amplifier in the amplification (or increase) of noise in processing and reading out of data, Silverbrook clearly teaches "a noisy read-out amplifier".

### ***Specification***

2. The disclosure is objected to because of the following informalities: The specification makes reference to the claims in various locations, such as pages 2-3. As an example, page 2, lines 25-30 refer to claim 3 and stating that claim 3 includes an encryption unit. However, claim 3 does not include any encryption

Art Unit: 2437

unit as the claims currently stand. Reference to the claims in the written description should be removed, so that there are no such issues in the future. Furthermore, the specification does not include the appropriate titles for sections thereof (e.g. "BACKGROUND OF THE INVENTION", "SUMMARY OF THE INVENTION", "BRIEF DESCRIPTION OF THE DRAWINGS", and DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS", or the like.

Appropriate correction is required.

### ***Claim Objections***

3. Claim 4 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. After the amendment to claim 1, claim 4 no longer further limits the parent claim, but rather states broader subject matter than that of claim 1 (in that claim 1 refers to the delay means comprising an analog noise source while claim 4 merely refers to the delay means as comprising a noise source with the same properties).

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claim 11 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 11 now refers to a "computer program product" and a "computer readable medium", however, neither are found within the application as originally filed. As will be described in the 101 rejection with respect to claim 11, not providing any description or definition regarding these limitations renders the claims non-statutory.

***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claim 11 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 11 is directed to "A computer program product embodied on a computer readable medium". The specification does not disclose what a computer program product is, nor what a computer readable medium is. This computer program product is clearly not statutory, even when "embodied on" a computer readable medium, for various reasons. Firstly, the computer readable medium is never described or defined, and therefore, is not limited to computer readable storage media. Next, this product

Art Unit: 2437

is not defined in any manner as to what it pertains other than the claim describing it as comprising "program code means for causing a computer to carry out the steps of the method as claimed in claim 10 when said computer program is run on said computer." These "program code means" are never even discussed, let alone defined in the specification. Furthermore, this "computer program product" is not stored on a computer readable storage medium.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claim 13 is rejected under 35 U.S.C. 102(e) as being anticipated by Silverbrook (U.S. Patent 6,757,832).

Silverbrook discloses an information carrier comprising an IC representing a physical unclonable function comprising:

An input means for receiving a challenge signal for challenging the IC (Figures 1-2; Column 27, line 45 to Column 28, line 23; and Column 34, line 64 to Column 35, line 45);

A response signal providing means for providing a response data signal in response to the challenge data signal (Figures 1-2; Column 27, line 45 to Column 28, line 23; and Column 34, line 64 to Column 35, line 45);

An output means for outputting the response data signal (Figures 1-2; Column 27, line 45 to Column 28, line 23; and Column 34, line 64 to Column 35, line 45); and

A delay means comprising a noisy read-out amplifier for amplifying the response signal provided by the response providing means, the delay means for delaying and/or prohibiting a provision and/or the output of the response data signal (Column 61, line 65 to Column 62, line 60; Column 76, line 64 to Column 77, line 22; Column 80, line 44 to Column 81, line 18; and Column 88, lines 10-22).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-6 and 8-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Silverbrook in view of Kocher (U.S. Patent 6,327,661).

Regarding Claim 1,



Silverbrook discloses an information carrier comprising an IC representing a physical unclonable function comprising:

An input means for receiving a challenge signal for challenging the IC (Figures 1-2; Column 27, line 45 to Column 28, line 23; and Column 34, line 64 to Column 35, line 45);

A response signal providing means for providing a response data signal in response to the challenge data signal (Figures 1-2; Column 27, line 45 to Column 28, line 23; and Column 34, line 64 to Column 35, line 45);

An output means for outputting the response data signal (Figures 1-2; Column 27, line 45 to Column 28, line 23; and Column 34, line 64 to Column 35, line 45); and

A delay means comprising a noise source for adding a noise signal to the response data signal provided by the response signal providing means, the delay means for delaying and/or prohibiting a provision and/or the output of the response data signal (Column 61, line 65 to Column 62, line 60; Column 76, line 64 to Column 77, line 22; and Column 80, line 44 to Column 81, line 18);

But does not explicitly disclose that the noise source is an analog noise source.

Kocher, however, discloses that the noise source is an analog noise source (Abstract; Column 4, lines 58-67; and Column 5, lines 38-60). It would have been obvious to one of ordinary skill

in the art at the time of applicant's invention to incorporate the leakage minimization techniques of Kocher into the authentication system of Silverbrook in order to allow the system to provide increased protection against attacks on the system by use of various entities and techniques, such as one or more digital and/or analog noise sources, clock skipping and internal clock rate modifying, random blinding of data, and/or random changes in operations to be performed, thereby making the system more secure against attacks.

Regarding Claim 9,

Claim 9 is an integrated circuit claim that corresponds to information carrier claim 1 and is rejected for the same reasons.

Regarding Claim 10,

Claim 10 is a method claim that corresponds to information carrier claim 1 and is rejected for the same reasons.

Regarding Claim 11,

Claim 11 is a computer program product claim that corresponds to information carrier claim 1 and is rejected for the same reasons.

Regarding Claim 2,

Silverbrook as modified by Kocher discloses the information carrier of claim 1, in addition, Silverbrook discloses that the response signal providing means comprises a memory for storing

pairs of challenge data and associated response data (Column 27, line 45 to Column 28, line 23; Column 34, line 64 to Column 35, line 45; and Column 80, lines 29-43).

Regarding Claim 3,

Silverbrook as modified by Kocher discloses the information carrier of claim 1, in addition, Silverbrook discloses that the response signal providing means comprises a response signal generation means for generating a response data signal in response to a challenge data signal (Column 34, line 64 to Column 35, line 45; and Column 80, lines 29-43).

Regarding Claim 4,

Silverbrook as modified by Kocher discloses the information carrier of claim 1, in addition, Silverbrook discloses that the delay means comprises a noise source for adding a noise signal to the response signal provided by the response signal providing means (Column 80, line 44 to Column 81, line 18; and Column 88, lines 10-22).

Regarding Claim 5,

Silverbrook discloses that the delay means comprises a noisy read-out means for amplifying the response signal provided by the response signal providing means (Column 80, line 44 to Column 81, line 18; and Column 88, lines 10-22).

Regarding Claim 6,

Silverbrook as modified by Kocher discloses the information carrier of claim 1, in addition, Silverbrook discloses that the delay means comprises analog limiting means for restricting the number of response data signals provided and/or outputted per time unit (Column 61, line 65 to Column 62, line 60; and Column 76, line 64 to Column 77, line 22); and Kocher discloses that the delay means comprises analog limiting means (Abstract; Column 4, lines 58-67; and Column 5, lines 38-60).

Regarding Claim 8,

Silverbrook as modified by Kocher discloses the information carrier of claim 1, in addition, Silverbrook discloses that the delay means comprises a counter means for limiting the total number of responses or the number of times the response to a given challenge can be provided, of the IC (Column 61, line 65 to Column 62, line 60; and Column 76, line 64 to Column 77, line 22).

Regarding Claim 12,

Silverbrook as modified by Kocher discloses the information carrier of claim 3, in addition, Silverbrook discloses that the signal generation means is an encryption unit (Column 34, line 64 to Column 35, line 45; and Column 80, lines 29-43).

8. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Silverbrook in view of Kocher, further in view of Miyaira (U.S. Patent 7,120,808).

Silverbrook as modified by Kocher discloses the information carrier of claim 6, in addition, Silverbrook discloses use of power control to stop power supply attacks (Column 85, lines 3-14; and Column 88, lines 46-48); but does not explicitly disclose limiting the amount of power available per time unit.

Miyaira, however, discloses limiting the amount of power available per time unit (Column 7, lines 55-67; and Column 10, lines 14-31). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the power control techniques of Miyaira into the authentication system of Silverbrook as modified by Kocher in order to allow the system to monitor and control power usage such that the system can throttle power usage when such usage reaches a threshold, thereby keeping power consumption within a predetermined range such that it is more difficult for an attacker to perform power supply attacks and attacks based on power consumption.

### ***Conclusion***

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Devadas (U.S. Patent Application Publication 2003/0204743).

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.**

Art Unit: 2437

See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2437

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham  
Examiner  
Art Unit 2437

/Jeffrey D Popham/  
Examiner, Art Unit 2437

/Emmanuel L. Moise/  
Supervisory Patent Examiner, Art Unit 2437